Office of the Governor
State Chief Information Officer

Security Policy and Guidelines

Title: Application Security Policy with Guidelines

Purpose: To ensure that the appropriate level of information security control is in place for applications.

As state agencies design, build and deploy information technology based services, each new project must address the security needed for the effective business operation of the information system. Security controls must be an integral part of project planning, development and implementation. Appropriate security controls may consist of both infrastructure and application elements.

Scope: This policy applies to all public agencies, their agents or designees subject to N.C.G.S. Article 3D of Chapter 147, "State Information Technology Services." Use by local governments, LEAs, community colleges, constituent institutions of the University of North Carolina and other public agencies is encouraged to the extent allowed by general statutes.

POLICY STATEMENT

All information technology services and systems developed or acquired by agencies subject to Article 3D of Chapter 147, "State Information Technology Services" must have documented security specifications that include an analysis of security risks and recommended controls (including access control systems and contingency plans). The system developer shall develop security specifications for approval by the agency[1] owning the system at appropriate points of the system development or acquisition cycle.

All information technology services and systems must address the security implications of any changes made to a particular service or system. The agencies must authorize all changes. Additionally, changes that impact the total state network must be approved by the State Chief Information Officer (State CIO).

GUIDELINES

The guidelines listed below may assist agencies as they consider security requirements during the planning, design, implementation, and operation of a new information technology service.[2] Information technology systems, services, and programs require different levels of security. All of the activities below may not be necessary for any given system or service.

---

[1] For purposes of this policy "agency" means the governmental entity with statutory authority for the information technology system.

[2] This conforms to the Information Technology Development Standards, Guides and Recommendation Practices adopted December 1, 1998.

I. PROJECT CONCEPT PHASE

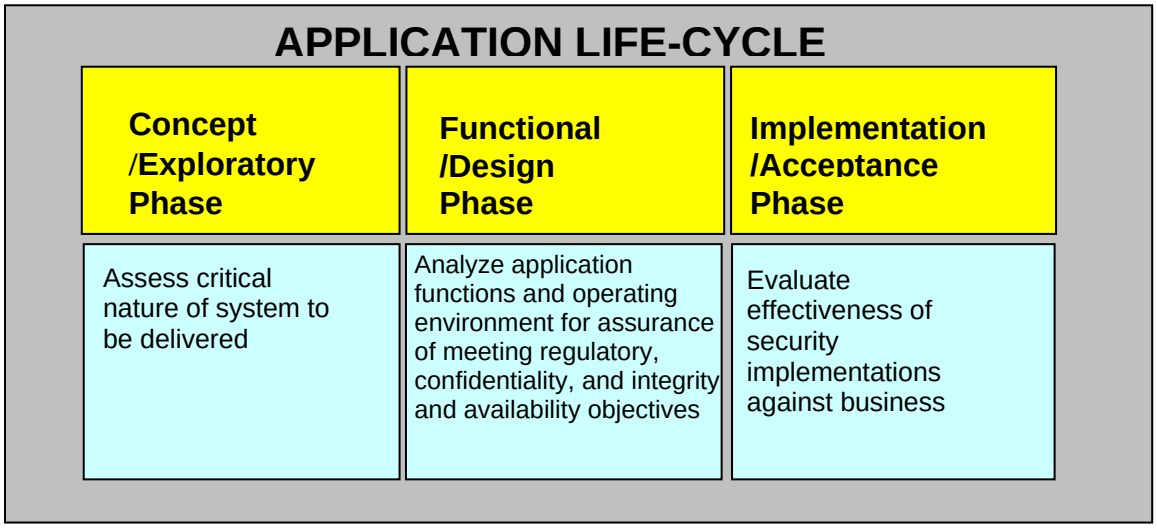
During the project concept phase, the agencies must perform a *risk assessment* of the proposed system to determine the appropriate level of security needed to meet the business requirements of the system. The specific project needs, including security, should be documented and approved by the agency.

II. PROJECT DESIGN PHASE

During the project design phase, the *business needs for security must be integrated into the system design*. The project's technology and the processes for using the system should be examined for their ability to support the confidentiality, integrity, authorization and availability objectives. The security considerations and recommended control measures should be documented in the project specifications and be approved by the agency.

III. IMPLEMENTATION/ACCEPTANCE PHASE

During the Implementation/Acceptance phase, the *test plan and testing results* are reviewed for assurance that the security measures satisfy the business requirements of the functional specifications.



I. PROJECT CONCEPT PHASE

SECURITY GUIDELINE ACTIVITIES	Date	By	References
Evaluate the business purpose of the system: a) Identify legal and policy requirements (*e.g.* Article 3D of Chapter 147, "State Information Technology Services" Security Policies, confidential personnel records to be accessed, environment for use) b) Identify potential losses arising from accidental or unauthorized activities, poor decisions based on unreliable information, or business costs due to system unavailability. c) Identify potential adverse customer reactions arising from system unavailability or unreliable information. d) Perform risk analysis. e) Document the issues identified. f) Agency approves security assessment work.			

II. PROJECT DESIGN PHASE

	SECURITY GUIDELINE ACTIVITIES	Date	By	References
A.	Conduct an analysis of the functional and design specifications to address the following concerns: a) Ensure individual accountability for all transaction actions. b) Ensure incoming data are complete, accurate, and authorized before completing the transaction action. c) Review/Label data confidentiality before granting access rights. d) Assign program function and data access privileges to users on a need-to-know basis and segregation of duties principle. e) Identify critical operations or confidential data that require special handling. f) Ensure auditability of transactions from origination to destination. g) Establish balancing controls to provide for a quick test of correctness of system actions. h) Ensure audit trails meet the business and/or regulatory requirements. i) Establish data retention/destruction requirements and provide backup/recovery elements and procedures to satisfy business continuity requirements for major and minor disruptions. j) Document security design and specification to ensure that they reflect § I. e). k) Agency approves design and specifications.			
B.	Analyze the operating environment (communications/computing hardware and software, programming languages, physical security and administrative procedures) to address the following concerns: a) Adequacy of physical and environmental controls for protecting computing equipment and information media. b) Availability requirements and risks associated with non-available resources; develop and exercise disaster recovery plans to mitigate risk commensurate with availability requirements. c) Sufficiency of authentication and access control mechanisms to ensure authorized access to system resources. d) Risks arising from transmissions of clear-text data and passwords and the need for encryption methods. e) Privileged program functions that need special handling. f) Privileged administrative duties such as system or database administration functions that required special treatment. g) Ensure that the access mechanism and procedure			

	restrict the processing of official data to authorized programs. h) Ensure that proper change control procedures are in place for promoting program changes to authorized status. i) Document analysis to ensure that it complies with § I.e). j) Agency approves analysis.			

III. IMPLEMENTATION/ACCEPTANCE PHASE

SECURITY GUIDELINE ACTIVITIES	DATE	BY	References
Review security implementation in the system acceptance phase: a) Verify that the risk analysis is documented in the system concept or exploratory phase and approved by the system owner and other stakeholders. b) Verify that security considerations and recommended control measures were documented in the functional/design phase and approved by the agencies. c) Verify that the system testing covers all recommended control measures specified in the system functional and design documentation. d) Verify that the testing effort is appropriate to fully test the security for the system. e) Document that the end product complies with § I. e). f) Agency approves security implementation.			

AUTHORITY

The State CIO has the authority to adopt this policy. G.S. §147-33.110